NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT

Debate VI: The Internet of Things is Blowing Up Everything - Service Providers, Carriers and the Cloud Industry Must Keep Calm and Carry On

Chaired by: Sathya Atreyam

WorldWide Research Manager Mobile and IoT Network Infrastructure

Panel:

Glenn Ricart, Founder & CTO, US Ignite

Milind Pansare, Director of Strategic Marketing, Aerohive Networks

Frank Wiener, VP Marketing, Wedge Networks

SATHYA ATREYAM

So, hello, everyone. I think the next topic dives into the Internet of Things. You will have seen the synopsis on your brochures that the Internet of Things is blowing up everything, but there is no reason to panic. We need to have a calm head. But just to set the stage for discussions here, I'll share a few slides and then I will invite the panel to share their thoughts on this topic.

As we see here in IDC, by no means this is the only view. I think all the other market research firms agree that it's a huge opportunity. But just to give a perspective, so we see this as a $1.46 trillion market opportunity and specifically, if you look at the regions, the United States, Western Europe are leading the pack, of course, followed by Japan and Asia Pacific which excludes Japan.

If you want to look at the industries which are driving this opportunity, yes, manufacturing, especially in the industry 4.0 in Western Europe is driving. But you can see here that there are multiple industry verticals which are driving this opportunity right from healthcare, discrete manufacturing to consumers, transportation, retail. So you name it, it's all here in that $1.46 trillion.

The next part was to highlight the actual unit economics is very important and if you look at this chart here, almost 150,000 devices will start connecting almost every minute by the year 2025. Right now it's almost like 5000 devices connecting every minute, so it's a massive shift in the next eight, nine years.

The next one was all these devices are going to generate data and that's going to be a data deluge. If you look at some of these curves here, almost 3.8 per cent of the data which will be generated is IoT relevant and IoT actionable is actually 8.6 times of the actual data which was generated. Totally, we are looking at almost 180 zettabytes by the year 2025. But it's a huge amount of data coming in.

Ecosystem. This slide just wants to give you a perspective of how many players and this is just the tip of the iceberg. But the key takeaway from this slide is it's an ecosystem. All of us have to work together to make this successful and we'll discuss a little bit on that.

Lastly, the third platform I think Tom Burns referred to the new platform from IDC's perspective. The third platform, technologies have four components. The cloud which will have variable endpoint workloads capability or scalability options, data, sovereignty, security, those are critical from a cloud perspective. From big data analytics, how do we make real time decisions there or create value-added content?

Social. It's still being discussed as how can the social be an outlet for automated responses to the consumers.

And most importantly, mobility. How do you connect remote endpoints, activate IoT applications? This is more of a success criteria which we feel from an IoT perspective we have to start thinking of cultivating ecosystems. You cannot no longer operate in a siloed fashion. You have to think about network as a resource on demand, when it is needed, where it is needed and specifically, enabling localisation. You know, access to the right information at the right time to the right enterprise or a consumer.

So with that being said a lot of things have to happen to make this successful. As much as this is giving a sense of panic, but this is a tremendous opportunity.

I think we have a very good panel here to discuss what can be done, what should be done, and I will introduce and you can expand on yourselves. Glenn Ricart from US Ignite, Milind Pansare from Aerohive and Frank Weiner from Wedge Networks, why don't you introduce yourselves, a little bit about your organisations.

GLENN RICART

I'm Glenn Ricart. US Ignite is an initiative of the United States government and also of 20 corporations to go and provide new applications in healthcare,

transportation, public safety, education that will help transform our cities globally in the next decade.

So we're a little bit ahead of some of the commercial companies you've heard talk at this conference so far. We're working on applying the basic research that is coming out of computer science labs, some of the newest ideas out of some of the corporate partners, and applying them in ways that help people. So it's those kinds of advanced applications we're really focused on.

SATHYA ATREYAM

Thank you. Milind.

MILIND PANSARE

Milind Pansare. I'm with Aerohive Networks and we do that first point of entry admission for IoT Devices into the network. So we provide the wireless LAN, if you will, the wireless access points and the switches and also partner with Dell on their switches. So we are looking at IoT from that perspective.

FRANK WIENER

I'm Frank Weiner with Wedge Networks. Wedge Networks is a cybersecurity solution provider. Just today we had a new product announcement. Yesterday you heard from Cylance and Stuart McClure, the CEO, talking about the role of artificial intelligence securing endpoints. What Wedge has done is we have licensed that technology and partnered with Cylance to introduce artificial intelligence in orchestrating that in combination with deep packet and deep content inspection so that we can secure data on the fly to secure the endpoints.

So bringing that back to IoT, by inspecting data in motion and detecting these threats in real time we add a layer of security to the Internet of Things as well as conventional computing devices.

SATHYA ATREYAM

I think I should thank them for participating because this covers pretty much most of the discussion of IoT in general, not just this panel, is the ecosystems of connectivity and most important, the security aspects.

So I would like to start with the connectivity discussions there. There is going to be a whole bunch of endpoints, a varied type of endpoint, but most importantly, varied types of technologies. You're talking about low power, VAN, LP-VANs there, the role of Wi-Fi and cellular. So would you like to comment on some of the connectivity challenges and opportunities per se? So maybe Glenn, if you could start from your perspective.

GLENN RICART

So, I love your charts. The Internet is about to be taken away from people and their web browsers and turned over to things. We're going to be outnumbered a hundred to one according to your chart in the use of the Internet. Is the Internet that we now have designed for and useful in that kind of arrangement? Most of the things that we're going to have are going to be smart have some kind of a local impact. They're going to go and change something in the local environment. They're going to be compared to other local sensors. They're going to be used for things that are mostly local.

So it's not clear that at any more makes sense to go things to a distant datacentre. The only reason we're going to a distant datacentre that's thousands of kilometres away is because of the economy of scale. But because of the numbers you just talked about, that scale is going to be local. So we're going to see the rise of sometimes called edge computing, local cloud computing. It's going to be cloud computing. It will be elastic just like cloud computing. A lot of the cloud computing things will still apply, but it's going to be local. That means that we're going to need to have a new structure for the Internet to support the Internet of Things in our communities.

So US Ignite is working on 15 cities in the United States to rewire them for east-west local traffic. We're installing digital town squares for local traffic exchange at very low latency and very high bandwidth to support the Internet of Things in these cities.

SATHYA ATREYAM

Great. Milind.

MILIND PANSARE

Just taking off on that point, if you think of the IoT, it's really networks of networks and there is a lot of intelligence at the edge and there is a lot of analytics and autonomous decision-making that can happen at the edge. Then there is certain things that you need to pull out. Not all traffic needs to flow back to one central point, so that actually brings up some interesting things, changes, for us on the networking side because if you look at wireless LAN networks, what's not important any more is the speed and feed of the devices themselves. What's important is actually making them more software-defined and adaptable networks and making them programmable with APIs so that you can actually start extracting out certain local intelligence and data.

Tom was speaking earlier. We also manage Dell switches, for example, so you can do unified wired and wireless policies because it's not just connection to the wireless for these IoT devices. They're also plugging into the edge

switchboards and taking power from there. So the switches are really actually becoming switches at the edge. They're power switches now top. There are less switches that do 60-watt power and they're powering LED lights as well and then there is traffic going back through Wi-Fi as well as through these switches.

So it's actually really interesting because you can do things right at the edge. We work with Statistica where you can now have analytics at the edge and so local decisions in a quick food restaurant, for example, about is my food spoiling because the sensor says the freezer is not at the right temperature and then when do I actually kick that back to corporate because that might be a brand issue if my franchisee isn't doing that. Those are two different kinds of discussions.

So I think that's really forcing a change to a software-defined approach to the LAN which is your wire and wireless access network. That's how we are approaching this.

SATHYA ATREYAM

Okay. Frank.

FRANK WIENER

When you're thinking about the connectivity of the Internet of Things, to your point, the key thing is if you're going to bring the Internet of Things and allow the innovation that it offers to come to life, the security officers in the enterprise have to allow it to happen. The interesting thing about the Internet of Things is it introduces new threat opportunities in at least two dimensions.

One is, is there the potential that somebody can hijack the Internet of Things and somehow take over its control to have direct effect that way.

The other is does it become a point of entry where they can move laterally to infect other things.

So, in order for the Internet of Things to come to life through connectivity we have to address the security aspects in order to achieve that full potential.

SATHYA ATREYAM

Yes. I think all three have raised very good points. I think from a security point of view, cellular traditionally has been very secure, but then Wi-Fi has its own challenges but opportunities. Then you have the ZigBees of the world, or Bluetooth coming in, or Beacon technology. So there will be a lot of opportunity for security solutions to play a role there.

I would like to start again now from Frank. Going into the core network point now from wireless, how do you see the security in terms of a vulnerability or visibility perspective? How are you seeing that?

FRANK WIENER

Certainly. So right now Wedge is actually working with a number of tier one mobile network operators. They not only want to secure the mobile smartphones, but they're looking at the Internet of Things as the next big connectivity market opportunity from their cellular infrastructure. Along with that, they not only want to provide the connectivity, but it goes back to the security side.

When you think about securing the Internet of Things, you either have to put security on the endpoint, or you have to secure it in the network when it's connecting to things. The challenge with putting it on the endpoint is there is a continuously evolving unlimited amount of endpoints that are always emerging. So always getting that security on the endpoint is going to be a challenge.

What these operators are doing is they're looking at can they offer security in their network on the fly so that the devices are protected whether they're running local security or not. That's where we're seeing a lot of energy go into the next big thing really.

SATHYA ATREYAM

From an enterprise perspective, I know Aerohive is focused on that. How do you see this security requirement coming?

MILIND PANSARE

With IoT, security is interesting because traditionally what Wi-Fi security has been about is you have enterprise authentication 21X. It's active directory-based. You come in, you authenticate yourself to the network and then what happens with devices that are now on these wireless LANS, they put them on PSKs, on a single shared PSK often on a single SSID. That's what happens even actually, strangely enough, on guest networks in the enterprise.

So, again, you need a software-defined approach because now you've got a sensor network. It's not just people. It's people and things and it's combinations of people and things that need to be authenticated. It's this person with this device at this time, so you need a security policy for that, or that set of sensors on that wall. So things like PSK, we've got these small little headless devices, unfortunately, that's how they run because that's all the intelligence they have, you actually have to have a layer above it so it looks

like PSK to that device but I can identify that device down to exactly where it is, shut it off. If I'm in a hospital, you can't take down 20 of these life support devices. You have no downtime. So can you with technologies like private PSK. So it has forced us to rethink.

When we talk about software defining this, it's not just software defining the application agility, but also identity and security and what that means when you have a sensor network as opposed to just a people network.

SATHYA ATREYAM

Glenn, I just wanted to point out, especially in terms of security, you had shared an interesting concept of network slicing. So maybe if you could throw some light as to how US Ignite is looking at this in the context of security.

GLENN RICART

Sure. Well we totally believe in the world is moving to software. We can write software and innovate it much more quickly than we can innovative hardware. So, commodity hardware with software that can evolve very quickly is going to be the dominant innovation methodology of the next decade.

As we do that let's think about how can we get to some radical securitisation that helps us in the security space and that radical securitisation that we're thinking of is why should we just have one Internet. Why don't we have two or five, or ten, or per application, or per enterprise? Well, we already do those things. We call them software-defined networks for VLANs or corporate enterprise networks and so forth. What if we extend that to things and applications of those things?

So, what we think of this as is not that we have 10,000 networks just like the businesses think of these brains that are parallel universes, but we think about slices of the physical and logical and overlaying networks that we now deal with. Those slices can be dedicated to devices or instances or various security domains.

So, the security might be focused much more on admission to one of those slices than it is to take a look at all traffic that is coming by some kind of inspection device.

I'm not saying that the inspection devices will go away. They will probably still be there too, but we think that admission into a slice is going to be one of the next new techniques that will add to our security portfolio.

SATHYA ATREYAM

Right. Interesting. I would like to now go into an ecosystem kind of discussion there. That's where I would like to start with. Glenn, you shared some things on the smart cities and how private and public organisations are collaborating. But from an ecosystem, developers play a critical role. How open is the system? How do you help the developers connect and create more applications? A few thoughts from a US Ignite point of view.

GLENN RICART

We're big believers in allowing everyone to innovate. We think that limiting innovation to any one player, any one carrier, any one enterprise manager is limiting the ability to innovate. So, just as we heard this morning from Dell about how they are separating their hardware from their software so you can have more software innovation, we believe you should do the same thing in the networking space.

So the folks who are providing network access ought to provide the ability to do software-defined programming of their networks. Oh, but you can't allow everyone to do software-define the carriers' network right, that would be crazy. Oh, unless you put it in a slice. Maybe you can programme your own slice, so software-defined networking for your slice of the carriers' network. So then you're ending up paying the carrier for the slice and then you are managing software-defined networking within that slice.

So that creates an ecosystem which is now open. We can now go and get the Apple developer group, the Google developer group, we can get students who are working in high school hackathons, we can get Code for America, we could get National Day of Civic Hacking, we can get them all involved in our cities and that's exactly what US Ignite is doing. We're trying to get all of those groups involved to go and help innovate for the benefit of their community.

SATHYA ATREYAM

Milind, from an enterprise point of view, you mentioned about retail or education. How do you see that developer community interacting and Aerohive's role in that?

MILIND PANSARE

I couldn't agree more with what Glenn just said. The key here is if you're providing, in this case, the edge network is to open it up with APIs. So we open it up with APIs that let you go all the way from identity, location and presence, configuration, monitoring. So just like we can create these. Networking companies have always created their own network management apps. What we have done is we've created a network management app as an

application over these APIs which really enables us to open up use cases like manned service providers maybe today offering Wi-Fi as a service, retailers, and there is people like Euclid Analytics or Cloud4Y. These are start-ups. Cloud4Y again serving the retail space with analytics and location presence.

But more interestingly, what will happen over time is nobody is ready to deal with configuring these networks yet. But the fact that you could actually reconfigure the network dynamically with config APIs could give, say, a logistics provider that millisecond advantage, or a carrier that certain advantage of trading. Think of the application.

So I think open APIs, it's happening right now and we are seeing ecosystems of vendors emerging. But what can happen with this, especially with the proliferation of devices and the data deluge that you talked about, is it's pretty amazing actually if you think about it.

SATHYA ATREYAM

Yes. Good point. Frank, from a Wedge Network perspective, I know there is the line rate yesterday we spoke about and today specifically security and Internet of Things. How do you see USA promoter of developer community there?

FRANK WIENER

Sure, sure. So in terms of innovating or enabling innovation and allowing folks to come together, a key part of that is obviously addressing the security which I already mentioned, which actually allows people to turn it on and use it.

But another part, and we were talking about this with Glenn earlier, and that is things like latency are really important. He talked about bringing stuff together to reduce distances and access to that. But along with that, the security aspects have to have incredibly low latency because some of these applications are not going to be very latency sensitive, but others are going to be extremely latency sensitive.

So being able to do policy enforcement and security enforcement with an eye toward latency and solutions that scale massively but also address the latency considerations are a key factor as well.

SATHYA ATREYAM

I think this has been very insightful from an ecosystem point of view and all the panellists have shared their specific organisations' contribution. I will open it up for questions from the floor in terms of what you have heard so far. Any questions.

GLENN RICART

We love questions.

SATHYA ATREYAM

There is one here on the front.

UNKOWN AUDIENCE PARTICIPANT

You say we love questions. In fact, I wanted to know the ideas a little bit more inside the ideas of the slices, the different slices of the network. That is to say that per slice you will have some type of system, for example, a slice just for security, a slice just for, I don't know, sections between the IP and a slice for video? What do you mean for this slice? In which direction are you looking for?

GLENN RICART

Well, you realise that I'm working kind of on the edge of new things. So I'm not in the commercial space. I'm looking at what is going to be happening in the future. The idea of slicing is really very flexible. I think we'll even talk some more about it in debate number eight. But I think that it could be used for any or all of those things and it remains to be seen exactly how we're going to do that.

In software-defined networking, the main principle is separating the management plane from the data plane. That's the main principle behind software-defined networking.

If you think of those as two different slices, you can now put that on the same infrastructure.

So it's a way of separating the infrastructure from the way that you use it in a way that allows for more innovation and exactly how that innovation gets used is going to depend.

In US Ignite right now in our prototypes we're putting in a slice per application. Each application gets its own slice. That slice gets different priorities, different treatment in quality of service. It gets different billing depending on what you're buying in that slice. You could buy a high priority low latency slice like Frank was talking about. That might be more expensive than a longer latency lower priority slice of the same size.

So right now we're experimenting with it in the application domain, but the domains you talk about may be just as valid. Maybe you would help us work that.

FRANK WIENER

Just to elaborate on that, prior to joining Wedge Networks I was with a company called Cyan acquired by Sienna. But we were very active in the SDN orchestration arena. One of the concepts that we socialised was the idea of taking the network and thinking of the network as a manufacturing production plant.

If you take the tech industry and you go back 20-some years, every company had their own manufacturing plant and they identified their product with their manufacturing plant. But the model shifted where everybody outsourced manufacturing because of the efficiency that you got by having folks who just focused on that one thing well.

But, if you take the network and think of it as a manufacturing plant but allow the people who want their services produced, or their products produced through that manufacturing plant where they're basically a slice of what's running in that larger manufacturing infrastructure, you can bring the same kind of economies to that infrastructure and efficiencies and get better products out.

GLENN RICART

And understanding and you can hypervise them separately.

FRANK WIENER

Exactly.

GLENN RICART

And you can go and scale these other technologies on a slice-by-slice basis, which is one of the reasons it's such an interesting building block.

SATHYA ATREYAM

It's the on demand era. Yes, next question.

ANTHONY CARUANA, CSO MAGAZINE

Thank you. Anthony Caruana, CSO Magazine. Just on the security side of IoT which you guys talked about quite extensively particularly from the network point of view, endpoint devices in IoT they vary very widely in their function. Some are just collection devices and are fairly dumb. Others are far

more sophisticated and are used for control, so they are reacting to stimuli. The threat environment is continually changing and I heard someone yesterday say they really just shuffle the deck chairs in their security book. But the reality is that the threats do change from time-to-time and threat actors alter their behaviours. We keep finding flaws in software. I keep hearing about this wonderful software-defined world we live in which seems to be a little bit more irresponsible than the hardware-defined world of the old days because the cost of software change is so low, or relatively low. Where does the responsibility of the device makers for IoT come into the picture because the network is great but what about the guys that are making these bits and pieces that were just sitting on our networks? Where is there responsibility start in the security game?

FRANK WIENER

Well I think the market is going to set expectations for device manufacturers to have certain levels of security. But obviously some of the devices just don't have the compute power to run a lot of that capability on its own.

ANTHONY CARUANA

Device makers are trying to make devices at one cent per device.

FRANK WIENER

Exactly. Exactly.

ANTHONY CARUANA

You can't secure one cent devices.

FRANK WIENER

Exactly and that's why the network that it connects to there has to be a network level component. The way you think about securing those devices is if you have a device that has very limited functionality, there are very limited numbers of commands and communications that should be going to and coming from that device.

So by inspecting it at the network layer where you're seeing the packets that are going in the content of the communications going on, you can ask the question of is this an appropriate communication or action associated with this device and limit the types of communications and activities to try to control that.

MILIND PANSARE

I think I have a similar perspective on this which is I buy these cheap devices that are made by Wirelesstag.net that cost next to nothing, you put one in your wine cooler it tells you what the temperature is and if anyone has opened the door. There is no way to secure that thing. But it's going to send something back, so that device manufacturer, I mean there is a thousand of these around, so actually do deep packet inspection because then security really becomes multi-layered here and then there has to be a holistic view across all the way back to the datacentre. But every piece of it has to do its bit. In the wireless LAN you have to do deep packet inspection right at that first point of admission and then you have to have secure GR eternals and the way to set up security policies so that that traffic can only go back and is the right kind of traffic. If it is outside the signature parameters, then it's not allowed and you can kill it right there. But it's multi-level and you need solutions like Wedge is talking about and then you will need approaches and abstractions like the slice abstraction that takes this to a more elegant level.

GLENN RICART

I was going to say that for things like your temperature sensor which don't have to report very often, so there is not a lot of volume of data, and wants to be very cheap, there is an interesting new idea I just wanted to share. That is that you go and have a set of pre-computed, so you don't have to have any expensive computation stuff on device, a table of things that it can go and say which is a one-time message. So if the temperature is 46º, it looks up and says what is the next one-time word I can use to mean 46º. Only if one of the words that is expected from that one-time list arrive at, for example, at your edge, you've now managed to secure that device without using any computation at all. You've done it with just a small bit of storage in these pre-stored words.

SATHYA ATREYAM

Yes. I think we are out of time. I think the next thing is a coffee break and you can definitely share something more.

But just to wrap up, I think there is a reality that this is an ecosystem and unless all of us co-operate right from devices to the network or the governments, this is not going to succeed there.

So with that being said, thank you to all your insights here and thank you for your participation.

GLENN RICART

Thank you Sathya. As you say, time to go for a cup of coffee, in some peoples' cases perhaps well needed. See you in about 15, 20 minutes.

[End]